

**BY ORDER OF THE COMMANDER
AIR FORCE SPACE COMMAND**



**AIR FORCE SPACE COMMAND
CHECKLIST 31-14**

3 FEBRUARY 2003

Security

INDUSTRIAL SECURITY (WING)

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: SFC (SSgt Glassic)
Supersedes AFSPCCL31-0014, 1 Oct 99.

Certified by: SF (Mr. James E. Moree)
Pages: 7
Distribution: F

This Checklist reflects Command requirements for Industrial Security offices to prepare for and conduct internal reviews.

SUMMARY OF REVISIONS

This checklist has been revised to update references and add commander and supervisor responsibilities. A bar (|) indicates a revision from previous edition.

1. References have been provided for each item. Critical items have been kept to a minimum and are related to public law, safety, security, fiscal responsibility, and/or mission accomplishment. While compliance with non-critical items is not rated, these items help gauge the effectiveness/efficiency of the function.
2. This publication establishes a baseline checklist. The checklist will also be used by the Command IG during applicable assessments. Use the attached checklist as a guide only. Add to or modify each area as needed, to ensure an effective and thorough review of the unit Industrial Security Program. **See Attachment 1**

MICHAEL W. HAZEN, Col USAF
Director of Security Forces

ATTACHMENT 1

INDUSTRIAL SECURITY (WING)

Table A1.1. Checklist.

MISSION STATEMENT: To ensure security and safeguarding of classified information and material provided to industry through inspection, oversight and training. NOTE: All references are from AFI 31-601, <i>Industrial Security Program</i> , unless otherwise stated.			
1. ESTABLISHING AN INDUSTRIAL SECURITY PROGRAM			
1.1. CRITICAL ITEMS:	YES	NO	N/A
1.1.1. Has the Installation Commander established contractor operations requiring access to classified information as intermittent visitors, visitor groups, or cleared facilities? (para 1.6.1.1.)			
1.1.2. Has the Installation Commander designated a Servicing Security Agency (SSA) (usually the Security Forces Information Security Office) to administer the Industrial Security Program? (para 1.6.1.4. and 1.6.5.1.)			
1.1.3. Is the SSA administering the Industrial Security Program and coordinating with the contracting office (CO), Cognizant Security Office (CSO), and other installation security discipline OPRs? (para 1.6.5.4.)			
1.2. NON-CRITICAL ITEM:	YES	NO	N/A
1.2.1. If the Installation Commander desires the Defense Security Service (DSS) security oversight for on-base contractor facilities, has a request been forwarded to DSS? (para 1.6.4.3.)			
2. SECURITY REVIEWS AND HOST SECURITY AGREEMENTS			
2.1. CRITICAL ITEMS:	YES	NO	N/A
2.1.1. Is the SSA conducting security reviews of cleared facilities and visitor groups with reviews sufficient in scope to monitor and evaluate compliance with contract specific requirements and pertinent National Industrial Security Program, DoD, & Air Force Industrial Security Program directives? (para 6.1.1. and 6.2.1.)			
2.1.2. Does the SSA ensure the contractor takes prompt corrective action when security program deficiencies are identified and promptly report security violations and/or compromises? (para 1.6.5.7.)			

2.2. NON-CRITICAL ITEMS:	YES	NO	N/A
2.2.1. If Installation Commander is conducting security reviews of on-base cleared facilities (using a designate SSA) has DSS been notified of this decision? (para 1.6.1.5.)			
2.2.2. Is DSS provided with facility surveys, security review reports and other related contract security documents? (para 1.6.5.8.)			
3. SCHEDULING INSPECTIONS			
3.1. CRITICAL ITEMS:	YES	NO	N/A
3.1.1. Is the SSA inspecting cleared facilities according to frequency schedules established by DoD and providing the cleared facility or visitor group management 30 days advanced written notification with the exception of conducting unannounced security reviews? (para 6.1.2)			
3.1.2. Is the SSA inspecting Visitor Groups according to frequency schedules established in DoD 5200.1-R, <i>Information Security Program</i> / AFI 31-401, <i>Information Security Program Management</i> ? (para 6.2.2.)			
4. OVERSIGHT REVIEWS AND REPORTING			
4.1. CRITICAL ITEMS:	YES	NO	N/A
4.1.1. Do Facility Clearance (FC) files contain all key documentation including DD Form 254, Contract Security Classification Specification, and related contract documents ? (para 6.1.3.2.)			
4.1.2. Does the ISPM, unit security manager, and integrated visitor group establish files and maintain all documentation as listed in AFI 31-601, para 6.2.4. thru 6.2.4.6.? (para 6.2.4.)			
4.1.2.1. Signed copy of DD Form 254 and any revisions? (para 6.2.4.1.)			
4.1.2.2. Signed copy of VGSA (optional for ISPMs)? (para 6.2.4.2.)			
4.1.2.3. Current listing of the key on base management officials or representatives? (para 6.2.4.3.)			
4.1.2.4. Copy of last annual program review? (para 6.2.4.4.)			
4.1.2.5. Copies of last two self-inspection reports (optional for ISPMs)? (para 6.2.4.5.)			

CRITICAL ITEMS Cont:	YES	NO	N/A
4.1.2.6. Copy of contractor visitor authorization letter (VAL). (Unit Security Managers will maintain a copy of each outgoing/incoming VAL generated by or directed to the integrated visitor group). (para 6.2.4.6.)			
4.1.3. Does the SSA keep copies of completed security review reports, pre-inspection visit memos and completed post-inspection correspondence for 2 years from date of the most recent inspection? (para 6.1.6.4. and 6.1.6.5.)			
4.2. NON-CRITICAL ITEM:	YES	NO	N/A
4.2.1. Within 10 days after completing a review, is the SSA forwarding a memo to the senior management official of the cleared facility addressing the following? (para 6.1.4.1.)			
4.2.1.1. Confirming contractor's security status as discussed during the exit review? (para 6.1.4.2.)			
4.2.1.2. Listing any deficiencies requiring corrective action? (para 6.1.4.3.)			
4.2.1.3. Requesting written confirmation on the status of any open major discrepancy within 30 days? (para 6.1.4.4.)			
5. REVIEWING VISITOR GROUPS			
5.2. NON-CRITICAL ITEMS:	YES	NO	N/A
5.2.1. For Visitor Groups operating under DoD 5200.1-R, <i>Information Security Program</i> / AFI 31-401, <i>Information Security Program Management</i> , requirements: does the AF activity limit the Visitor Group's access to "need to know" contract-specific performance information only? (para 5.2.1.)			
5.2.2. Does the Visitor Group Security Agreement clearly reflect the AF is accountable for and controls all classified information? (para 5.2.4.)			
5.2.3. If Visitor Groups are using the Automated Information System (AIS) to process classified information, is the system an approved AF AIS system or network? (para 9.1.2.)			

6. UNSATISFACTORY REVIEW			
6.1. CRITICAL ITEMS:	YES	NO	N/A
6.1.1. Does the SSA assign an unsatisfactory rating when: (para 6.1.5.1.)			
6.1.1.1. A cleared facility/visitor group fails to satisfactorily perform its contractual security responsibilities? (para 6.1.5.1.1.)			
6.1.1.2. Major failures in the contractors security program have resulted in or could reasonably be expected to result in the loss or compromise of classified information? (para 6.1.5.1.2.)			
6.1.1.3. The contractor is clearly responsible for the security problems cited during a periodic security review? (para 6.1.5.1.3.)			
6.1.2. Does the SSA coordinate with the CSO and base-contracting officer when assigning an unsatisfactory security review rating? (para 6.1.5.1.4.)			
6.1.3. When assigning an unsatisfactory rating, is the SSA notifying the HOF through the contracting office requesting prompt and complete corrective action? (para 6.1.5.1.5.)			
7. CONTRACTS			
7.1. NON-CRITICAL ITEMS:	YES	NO	N/A
7.1.1. Does the SSA maintain contract folders on each cleared facility and visitor group having access to classified information? (para 1.6.5.5.)			
8. DD FORM 254			
8.1. NON-CRITICAL ITEMS:	YES	NO	N/A
8.1.1. Is the SSA reviewing draft DD Form 254's and draft security classification guides. Is the SSA review and coordination shown in DD Form 254, block 13? (para 1.6.5.3./4.2.3.)			
8.1.2. When DSS is no longer responsible for security oversight of cleared facilities involved in SCI or SAP's, is a copy of DD Form 254 sent to HQ DSS? (para 4.4.1.)			
8.1.3. Are all known contract performance locations specified on the DD Form 254 and are copies of applicable DD Form 254 forwarded to SSA's at each performance location? (para 4.4.2.)			

9. REVIEWING AND CERTIFYING DD FORM 254			
9.1. NON-CRITICAL ITEMS:	YES	NO	N/A
9.1.1. Is the serving SSA reviewing the DD Form 254 to ensure the security classification guidance is accurate, approved, and appropriate? (para 4.3.1.)			
9.1.2. Is DD Form 254 certified by the contracting officer? (para 4.3.3.)			
10. AIR FORCE VISITS TO CONTRACTORS			
10.1. NON-CRITICAL ITEM:	YES	NO	N/A
10.1.1. Do Air Force personnel who require access to classified information while visiting contractor facilities comply with the provisions of DoD 5200.1-R and the National Industrial Security Program Operating Manual (NISPOM)? (para 7.4.)			
11. FACILITY CLEARANCES			
11.1. NON-CRITICAL ITEMS:	YES	NO	N/A
11.1.1. When requesting an interim Top Secret Facility Clearance (FCL), do contracting officers prepare and route FCL sponsorships through command channels to the MAJCOM, FOA, or DRU commander for approval and do these requests include the following? (para 2.1.2.)			
11.1.1.1. An explanation why an interim Top Secret FCL would prevent a crucial delay in the award or performance of a classified contract? (para 2.1.2.1.)			
11.1.1.2. A list giving the legal name of the facility seeking sponsorship, its complete street address, and the names and positions of people who are applying for interim Top Secret authorization? (para 2.1.2.2.)			
11.1.1.3. The address of the authorizing DSS? (para 2.1.2.3.)			
11.1.2. Is the SSA conducting surveys and administrative inquiries of the FCL as requested by the CSO, and ensuring contractor compliance with the (NISPOM)? (para 2.1.3.2.)			

NON-CRITICAL ITEMS Cont:	YES	NO	N/A
11.1.3. Does the SSA complete the FCL survey using DD Form 374, DoD Facility Security Clearance Survey Data Sheet , or the Core Data Input Sheet (CDU), and is a copy provided to the CSO? (para 2.1.3.3.)			
11.1.4. INVALIDATING FACILITY SECURITY CLEARANCE			
11.1.4.1. Is the CSO notifying contracting officers in writing when the FCL of a contractor is invalidated?(para 6.1.6.1.)			
11.1.5. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI)			
11.1.5.1. Does the CSO notify contracting officers when a contractor performing on a classified contract has FOCI? (para 2.2.1.)			
11.1.6. REPORTING COMPROMISE AND OTHER SECURITY VIOLATIONS			
11.1.6.1. Are on-site/on-base contractors following the NISPOM, DoD, and Air Force instructions when reporting the loss, compromise, and possible compromise of classified materials? (para 1.8.2.1.)			
11.1.6.2. Does the installation commander follow the instructions by DoD 5220.22-R, Industrial Security Regulation , to report the loss, compromise, or possible compromise of classified information for on-base contractor operations for which the Air Force has security oversight? (para 1.8.5.1.)			
11.1.6.3. Is the Air Force activity, CSO and the contractor notified of decisions to declassify, downgrade, or retain the security classification of the affected material? (para 1.8.5.4.)			
11.1.6.4. Does the SSA report cases of espionage or sabotage involving visitor groups or cleared facilities to the serving AFOSI? (para 1.8.3.1.)			
11.1.7. INTERNATIONAL SECURITY REQUIREMENTS			
11.1.7.1. If a contractor requests permission to submit a request to disclose classified information to a foreign interest, is the request forwarded through command channels IAW AFI 16-201, Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations ? (para 11.3.)			